National Infrastructure Protection Center CyberNotes

Issue #2000-13 *July 3, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 15 and June 29, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
BEA Systems[1] Windows 98/NT 4.0/2000, Unix	WebLogic Express & Server 3.1.8, 4.0x, 4.5x, 5.1x	A show code vulnerability exists, which could allow a malicious user to view the source code of any file within the web document.	For a workaround, see the WebLogic Server Configuration documentation located at: http://www.weblogic.com/docs51/admindocs/lockdown.html#1111303	WebLogic Source Code Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Foundstone, Inc. Security Advisory, FS-062100-4-BEA, June 21, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Cisco Systems[2] ***Cisco warns customers about this vulnerability.***[3] ***This vulnerability has been discussed previously in CyberNotes.***	**IOS Software 11.3AA, 12.0 releases: 12.0(2) up to and including 12.0(6) and 12.0(7)**	**A vulnerability exists in the Telnet Environment handling code, which causes the Cisco router to reload unexpectedly when the router is tested for security vulnerabilities by security scanning software programs. The defect can be exploited repeatedly to produce a sustained Denial of Service attack.**	**For a workaround, see the Cisco Security Advisory on this issue at: http://www.cisco.com** ***Cisco customers using the affected IOS software releases – including 11.3AA, and a number of 12.0 releases up to and including 12.0(6) – are urged to upgrade as soon as possible to later versions, which are not vulnerable to the defect.*** ***Users running Cisco IOS software versions 11.3, 11.3T, 11.2 or lower and 12.0(8) or 12.1 or higher are not affected.***	**Cisco IOS Software TELNET Option Handling**	**Low/ High** **(High if DDoS best-practices not in place)**	**Bug discussed in newsgroups and websites. Numerous security scanners are available and carry out this attack.** ***This vulnerability has appeared in the Press and other public media.***
DalNet[4]	IRCD 4.6.5	A buffer overflow vulnerability exists in the 'summon' command, which could grant a remote malicious user access on the host (with the privileges of the server).	No workaround or patch available at time of publishing.	IRCD Server 'Summon' Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Debian[5] Unix	CUPS 1.0.3 and prior CUPS 1.0.5	A Denial of Service vulnerability exists in certain versions of the CUPS (Common UNIX Printing System), which could result in disruption of print services.	Patches available at: http://www.debian.org/~licquia/cupsys_1.0.4-7_i386.deb http://www.debian.org/~licquia/cupsys-bsd_1.0.4-7_i386.deb http://www.debian.org/~licquia/libcupsys1_1.0.4-7_i386.deb http://www.debian.org/~licquia/libcupsys1-dev_1.0.4-7_i386.deb	CUPS Denial of Service	Low	Bug discussed in newsgroups and websites.
Deerfield.com[6] Windows 95/98/NT 4.0	Alt-N MDaemon 2.8.50	A Denial of Service vulnerability exists due to the mishandling of POP3 commands by the MDaemon.	Alt-N has rectified this issue in MDaemon V2.8.6.0 and all later versions.	MDaemon Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Floosietek[7] Windows 95/98/NT 4.0	FTGate 2.2	A vulnerability exists which could let a malicious user bruteforce usernames and passwords.	No workaround or patch available at time of publishing.	FTGate Mail Server	Medium	Bug discussed in newsgroups and websites.

[2] Cisco Security Advisory, CI-00.03, April 19, 2000.
[3] Vnunet.com, June 6, 2000.
[4] SecurityFocus, June 28, 2000.
[5] Securiteam, June 22, 2000.
[6] Securiteam, June 20, 2000.
[7] Bugtraq, June 26, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Flowerfire[8] Unix	Sawmill 5.0.21	Two security vulnerabilities exist: one gives access to local files; and the other enables remote malicious users to easily retrieve the administrator password.	No workaround or patch available at time of publishing.	Sawmill File Access and Weak Password Encryption	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Fortech[9] Windows 95/98/NT 4.0/2000	Proxy+ 2.40	A vulnerability exists, which could allow a malicious user to bypass the remote administration restriction.	No workaround or patch available at time of publishing. Unofficial workaround (Securiteam): Enable HTTP Basic authentication instead.	Proxy+ Telnet Gateway	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
GlFtpd[10]	GlFtpd 1.18-1.21b8	A vulnerability exists in the access-checking feature of the privpath directive, which could allow a malicious user to download sensitive information they are not privileged to.	This vulnerability was fixed in version 1.21 of GlFtpd, available at: http://glftpd.deepwell.com	GlFtpd Privpath Directive	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[11] Unix	MPE/iX 4.5, 5.0, 5.5, 6.0, 6.5	A vulnerability exists which could let a malicious user escalate his or her privileges.	Temporary Workaround: Secure DBUTIL.PUB.SYS and your database schemas with a lockword.	HP TurboIMAGE DBUTIL Privilege Elevation	Medium	Bug discussed in newsgroups and websites.
IBM[12] Unix	AIX 4.3, 4.3.1, 4.3.2	A vulnerability exists in the cdmount program, which could allow a malicious user to execute commands with root privileges.	An advisory from IBM is provided below. A suitable workaround is to remove the setuid bit from the cdmount binary. IBM AIX 4.3.2: http://service.software.ibm.com/support/rs6000 IBM AIX 4.3.1: http://service.software.ibm.com/support/rs6000 IBM AIX 4.3: http://service.software.ibm.com/support/rs6000	AIX Cdmount Insecure External Program Call	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
iMesh.Com[13] Windows 95/98/NT 4.0/2000	iMesh 1.02 and previous	A buffer overflow vulnerability exists which could allow the execution of arbitrary code.	No workaround or patch available at time of publishing.	iMesh Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[8] Bugtraq, June 27, 2000.
[9] Securiteam, June 29, 2000.
[10] Bugtraq, June 26, 2000.
[11] Hewlett-Packard Advisory, 0007, 26 June 2000.
[12] Securiteam, June 22, 2000.
[13] BluePanda Vulnerability Announcement, June 26, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
International TeleCommuni-cations[14] Windows NT 4.0	WebBBS 1.1.5	A buffer overflow vulnerability exists in the web server, which could allow a malicious user to execute arbitrary code.	International Telecommunications has addressed this issue in WebBBS 1.17. Official shareware release date for this version is July 1, 2000.	WebBBS Web Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[15] Windows 95/98/NT 4.0/2000	Internet Explorer 5.0, 5.01; Outlook 97.0, 98, 2000; Outlook Express 5.0	A security vulnerability exists which enables a remote malicious user to force a file onto the target computer.	No workaround or patch available at time of publishing.	Internet Explorer and Outlook/ Outlook Express Remote File Write	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[16] Windows 95/98/NT 4.0/2000	Internet Explorer 5.01; Access 2000	A vulnerability exists which could permit remote malicious execution of Visual Basic for Applications (VBA) code through web pages or HTML e-mail messages utilizing IFRAME without a user's consent or acknowledgment.	No workaround or patch available at time of publishing.	Internet Explorer and Access 2000 VBA Code Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[17] Windows 95/98/NT 4.0/2000	PowerPoint 2000; Internet Explorer 5.01	A vulnerability exists which could allow the execution of programs when viewing a web page or HTML e-mail, which in turn could provide full control of a targeted computer.	Unofficial Workaround (Georgi Guninski): Disable Active Scripting or Disable Run ActiveX controls and plug-ins	Internet Explorer and Excel/ PowerPoint 2000 ActiveX Object Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[18] Windows 95/98	Windows 95, 98	A vulnerability exists in the way Windows 9x handles spoofed ARP packets sent out on a network, which could allow a malicious user to reroute traffic intended for specific hosts to any other machine on the same subnet as the target.	No workaround or patch available at time of publishing.	Windows 9x ARP Spoofing	Medium	Bug discussed in newsgroups and websites.

[14] Delphis Consulting Plc Security Team Advisories, DST2K0018, June 19, 2000.
[15] Securiteam, June 27, 2000.
[16] Georgi Guninski Security Advisory #14, June 27, 2000.
[17] Georgi Guninski Security Advisory #13, June 27, 2000.
[18] Bugtraq, June 29, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[19] Windows NT 2000	Windows NT 2000 Professional, Server, Advanced Server	A security vulnerability exists which could allow a malicious user to gain additional privileges on a machine after keyboard login.	Patch available at: http://download.microsoft.com/download/win2000platform/Patch/Q260197/NT5/EN-US/Q260197_W2K_SP1_x86_en.EXE This patch should not be applied to clustered Windows 2000 systems that are administered through the Microsoft Management Console.	Windows 2000 Desktop Separation	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[20] Unix	Allaire JRun 2.3.x	A number of vulnerabilities exist when the documentation, sample code, examples, and applications as well as tutorials (shipped with JRun) are present on the host server.	Workaround: Until the next version of JRun is released, Allaire strongly recommends removing all documentation, sample code, examples, and tutorials from production servers. All files should be removed from the directories JRUN_HOME/servlets and JRUN_HOME/jsm-default/services/jws/htdocs. The Security Best Practice article on "Removing Sample Applications and Online Documentation from Production Servers" is available at: http://www.allaire.com/Handlers/index.cfm?ID=16258&Method=Full	Allaire JRun 2.3.x Sample Files	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[21] Unix	Caldera OpenLinux 2.2-2.4; Conectiva Linux3.0, 4.0, 4.0es, 4.1, 4.2, 5.0; Debian GNU/Linux 2.1-2.3; Red Hat Linux 6.1, 6.2; Slackware Linux 7.0, 7.1; Washington University wu-ftpd 2.4.2, 2.5, 2.6	A security vulnerability exists which could allow remote malicious users to gain root access. Anonymous ftp is exploitable making it even more serious as attacks can come anonymously from anywhere on the Internet.	Contact your vendor for the patch.	Wu-Ftpd Remote Format String Stack Overwrite	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published. ***This vulnerability has appeared in the Press.***

[19] Microsoft Security Bulletin, MS00-020, June 15, 2000.
[20] Allaire Security Bulletin, ASB00-15, June 22, 2000.
[21] Securiteam, June 24, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[22] Unix	Debian Linux 2.1, 2.2; ISC DHCP Client 2.0, 3.0b1	A vulnerability exists which allows for remote exploitation by a corrupt DHCP server (or a malicious user pretending to be a DHCP server) which could allow root access.	ISC has released patched versions, 2.0pl1 and 3.0b1pl14. which are available at: ftp://ftp.isc.org/isc/DHCP The reported vulnerability is fixed in the package DHCP-client-beta 2.0b1pl6-0.3 for the current stable release and in DHCP-client available at: http://security.debian.org/dists/stable/updates/	ISC DHCP Client Remote Root	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[23] Unix	KDE 1.1, 1.1.1, 1.1.2, 1.2, 2.0 BETA; Open Group X 11.0R6, 11.0R6.1, 11.0R6.2, 11.0R6.3; Wings wdm 1.2; XFree86 X11R6 3.3.3-3.3.6, 4.0	A buffer overflow exists in xdm and its derivatives, including kdm and wdm, which make it possible to perform a remote buffer overflow or crash xdm.	No workaround or patch available at time of publishing.	xdm/kdm/wdm Buffer Overflow	Low	Bug discussed in newsgroups.
Multiple Vendors[24] Unix	kon2-0.3.9	KON2 (Kanji On Console) allows viewing of Japanese fonts on the Linux console. This package contains two exploitable buffer overflows, which may lead to a root compromise.	No workaround or patch available at time of publishing.	KON2 Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[25] Unix	Open Group X 11.0R6.1, 6.2, 6.3, 6.4; XFree86 X11R6 3.3.3, 3.3.4, 3.3.5, 3.3.6, 4.0; RedHat Linux 6.1, 6.2	Various security-coding flaws exist in libX11. These flaws can be used to gain root privileges, cause a Denial of Service attack, and depletion of system resources.	No workaround or patch available at time of publishing.	XDMCP Infinite Loop Denial of Service	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[26] Unix	XFree86 X11R6 3.3.3-3.3.6, 4.0; Open Group X 11.0R5, 6, 6.1-6.4; GNOME 1.0.x, 1.1	Due to inadequate bounds checking in LibICE, a Denial of Service vulnerability exists.	No workaround or patch available at time of publishing.	LibICE Denial of Service	**Low/High** **(High if DoS best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit script has been published.

[22] Securiteam, June 28, 2000.
[23] Bugtraq, June 20, 2000.
[24] Bugtraq, June 19, 2000.
[25] Securiteam, June 26, 2000.
[26] Securiteam, June 27, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netnation Communi-cations Inc.[27] Unix	Secure Locate 2.0, 2.1	A vulnerability exists due to improper validity checking in the LOCATE_PATH environment variable, which could allow a malicious user the ability to construct an invalid LOCATE_PATH variable, which could cause an exploitable SEGV in slocate.	Upgrade available at: ftp://ftp.mkintraweb.com/pub/linux/slocate/src/slocate-2.2.tar.gz Kevin Linsday, the author of Secure Locate, released this upgrade.	Secure Locate LOCATE_ PATH Validation	Low	Bug discussed in newsgroups and websites.
Netscape[28] Unix	Netscape Professional Services FTP Server 1.3.6	Due to the failure of the FTP server to enforce a restricted user environment (chroot), vulnerability exists which may lead to a remote or local root compromise.	No workaround or patch available at time of publishing.	Netscape Professional Services FTP Server	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Netwin[29]	DMailWeb & CWMail 2.53, 2.6g, 2.6I, 2.6j	A series of vulnerabilities related to unchecked user supplied data (overly long strings etc.) exist which could result in a Denial of Service.	New versions of DMailWeb (and CWMail) can be downloaded from: ftp://ftp.netwinsite.com/dmailweb	DMailWeb & CWMail Multiple Denial of Service	**Low/High** **(High if DoS best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
Netwin[30]	Netwin DMailWeb & CWMail 2.6g	Denial of Service vulnerabilities exists which could give a malicious user the ability to flood the SMTP service used by the mail server or login and send mail without being a registered user.	Netwin's DMailWeb & CWMail Server version 2.6i and 2.6j both address this issue located at: http://www.netwinsite.com	DMailWeb & CWMail Denial of Service	**Medium/ High** **(High if DoS best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
Network Associates[31]	Net Tools PKI Server 1.0	Remotely exploitable buffer overflows and the potential for the execution of arbitrary commands exist.	Network Associates has released the following hotfix which eliminates this vulnerability at: ftp://ftp.tis.com/gauntlet/hide/pki/PKISERVER100-SP1-103-1.EXE	Net Tools PKI Unauthenti-cated Access and Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
NetworkICE[32] Windows 95/98/NT 4.0/2000	BlackICE Defender 2.1 and previous; BlackICE Agent 2.0.23 and previous	At security level NERVOUS or lower, BlackICE and the host protected by BlackICE are vulnerable to Back Orifice (BO) 1.2.	No workaround or patch available at time of publishing. Unofficial workaround (Securiteam): Configure BlackICE to the PARANOID setting which will block all incoming UDP and TCP connections or implement an antivirus program.	BlackICE High UDP Port Block Delay	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[27] Bugtraq, June 21, 2000.
[28] Securiteam, June 24, 2000.
[29] Bugtraq, June 21, 2000.
[30] Bugtraq, June 23, 2000.
[31] Bugtraq, June 18, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Novell[33]	Netware 5.0, 5.1 Netscape Enterprise Server for NetWare 4/5 4.1.1, 4/5 5.0	A buffer overflow exists in the Netscape Enterprise Server for Netware, which could allow the execution of arbitrary code.	Patch available at: Novell Netware 5.1: http://support.novell.com/servlet/filedownload/pub/e51sp1.exe	Netscape Enterprise Server for Netware Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Panda Software[34]	Panda Antivirus for NetWare 2.0	Port 2001 is open by default, which will allow a remote malicious user to execute any NetWare command via the 'CMD' option.	Panda Software included a fix for this vulnerability with the June version of the Global Virus Insurance disk (M6/A00).	Panda Remote Unauthenti-cated Administration	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[35] Unix	RedHat gkermit 1.0-3	A vulnerability exists in the gkermit binary (released after February 27, 2000), which could let a malicious user gain access to any files that are readable by the UUCP user.	No workaround or patch available at time of publishing.	Gkermit Setgid UUCP	Medium	Bug discussed in newsgroups and websites.
Sapporo Works[36] Windows 95/98/NT 4.0/2000	WinProxy 2.0, 2.0.1	A security vulnerability exists which enables remote malicious users to shut down the server. This request can cause anything from a Denial of Service attack to arbitrary code execution (and gain of administrative privileges).	Upgrade to version 2.0.2 which is located at: http://homepage2.nifty.com/spw/winproxy/download.html	WinProxy Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Shadow Op Software[37]	Dragon Server 1.0, 2.0	Multiple Denial of Service vulnerabilities exist due to improper bounds checking.	No workaround or patch available at time of publishing.	Dragon Server Multiple Denial of Service Vulnerabilities	**Low/High (High if DoS best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
Silicon Graphics Inc. [38] Unix	Workshop Debugger and Performance Tools 2.6 and lower	A vulnerability exists in cvconnect(1M), which will allow a malicious user to overwrite any file on the system.	This issue has been corrected in WorkShop 2.7 and higher.	IRIX Cvconnect File Overwrite	**High**	Bug discussed in newsgroups and websites.

[32] Securiteam, June 21, 2000.
[33] Bugtraq, June 26, 2000.
[34] Infosec Security Vulnerability Report, Infosec.20000617, June 17, 2000.
[35] Bugtraq, June 21, 2000.
[36] SPS Advisory #37, June 27, 2000.
[37] USSR Advisory Code, USSR-2000046, June 16, 2000.
[38] Silicon Graphics Inc. Security Advisory, June 20, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Veritas Software[39] Unix	Volume Manager 3.0.2-3.0.4	A security vulnerability exists which can, under specific circumstances, allow malicious users to gain root access.	The vendor indicates that the problem has been remedied in beta versions of Volume Manager 3.1. Unofficial workaround (Bugtraq) Add the following line to the beginning of the /etc/rc2.d/S96vmsa-server file: *umask 022*	Volume Manager File Permission	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Zope[40, 41] Unix	Zope 2.1.x, 2.2 beta1	A security vulnerability exists that involves an inadequately protected method in one of the base classes in the DocumentTemplate package that could allow the contents of DTMLDocuments or DTMLMethods to be changed remotely or through DTML code, without forcing proper user authorization.	Zope 2.1.7 release has been made that resolves this issue for Zope 2.1.x users. This release is available from Zope.org: http://www.zope.org/Products/Zope/2.1.7/ A patch is also available if it is not feasible to update your Zope installation at this time (the patch is based on 2.1.6): http://www.zope.org/Products/Zope/2.1.7/DT_String.diff Users of Red Hat Powertools 6.1, upgrade to the version of Zope released in Red Hat Powertools 6.2 (2.1.2-5) at: ftp://ftp.redhat.com/pub/redhat/powertools/6.2/	Zope DTML Templates And DTML Methods Remote Modification	Medium	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between June 15 and June 29, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or**

[39] Securiteam, June 18, 2000.
[40] Bugtraq, June 16, 2000.
[41] RedHat, Inc. Security Advisory, RHSA-2000:038-01, June 22, 2000.

patches, or which represent scripts that hackers/crackers are utilizing. During this period, 55 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
June 29, 2000	Ex_winproxy.c	WinProxy 2.0.0/2.0.1 contains many remotely exploitable buffer overflows, including an exploit for the POP3 service which has been tested on Japanese Windows 98.
June 29, 2000	Format_bugs.txt	Format Bugs - What they are, where they came from, and how to exploit them. Includes code samples and debugger output.
June 29, 2000	Ie5.force-feed.txt	Technique for manually forcing a file onto a target computer, running Microsoft Internet Explorer 5 and accompanying mail and news clients on Windows 95/98/2000.
June 29, 2000	Ie5-access2000.txt	Exploit code for the Internet Explorer 5.01 and Access 2000 vulnerability.
June 29, 2000	Ie5-excel-powerpoint.txt	Technique for exploiting the Internet Explorer 5.01, Excel 2000, and PowerPoint vulnerability.
June 29, 2000	**Imbof102.txt**	**Technique for exploiting the iMesh 1.02 Windows buffer overflow vulnerability, which allows the execution of arbitrary code.**
June 29, 2000	Lsof_4.50_W.tar.gz	Powerful Unix diagnostic tool.
June 29, 2000	NScan0666b11f.zip	Portscanner for Windows (up to 200 ports per second) for both hosts and large networks with numerous features: it scans not only address ranges, but also files with host lists (e.g. proxy list, domain zone or old log). It includes a set of additional tool in the pack: whois client, very fast traceroute, and a TCP-based DNS client that supports most of the available options including AXFR zone transfer.
June 29, 2000	Rvscan.v3-b1.tgz	Shell script based Unix remote vulnerability scanner which is based on fts-rvscan but has many new additions, such as 100 new cgi checks, new bind checks, ftpd checks, BSDI vulnerabilities, more rpc checks, Solaris vulnerabilities, new pop3 checks, bootp and mdbms, more sendmail checks, and better logging. It does a very thorough job, even includes some non-published exploit checks.
June 29, 2000	Suidbofcheck.pl	Perl script which searches the system for suid binaries in /usr/bin, /bin, /sbin, and /usr/sbin and tests each one against a standard buffer overflow (both with and without the use of environmental variables).
June 29, 2000	Wingate.py	Denial of Service exploit for the Qbik Wingate 3.0. vulnerability.
June 28, 2000	**dalnet465partial-exp.c**	**Exploit script for the DalNet IRC Server 'Summon' Buffer Overflow vulnerability.**
June 28, 2000	Ffbtester-2.0B-20000628.tar.gz	A utility for doing quick, proactive security checks of binary programs by performing checks of single and multiple argument command line overflows and environment variable overflows.
June 28, 2000	KNmap-0.7.2.tar.gz	New KDE front-end for Nmap which supports all the scan methods and a great deal of options.
June 28, 2000	Saint-2.1.1.beta2.tar.gz	A security assessment tool based on SATAN.
June 28, 2000	SING-1.0b7.tgz	SING sends fully customized ICMP packets from the command line. It is a replacement for ping which adds certain enhancements such as fragmentation, send/read spoofed packets, sends many ICMP types (Address Mask, Timestamp, Router Discovery, etc) and Error (Redirect, Unreach, Time Exceeded), oversize packets, etc.
June 28, 2000	Smit.tar.gz	Smit is a simple ARP hijacking tool for switched and unswitched networks.
June 27, 2000	**Dehash-sawmill.c**	**Exploit script for the Sawmill File Access and Weak Password Encryption vulnerability.**

Date of Script (Reverse Chronological Order)	Script Name	Script Description
June 27, 2000	**Icebreak.c**	**Exploit script for the LibICE Denial of Service vulnerability.**
June 27, 2000	Isc-dhcpd.exploit.txt	Exploit technique for the ISC DHCP client vulnerability.
June 27, 2000	Leafchat.dos	Java source to remotely crash LeafChat clients.
June 24-26, 2000	2dopewars_exploits.exe	Technique for exploiting the security vulnerabilities in Dopewars 1.47-current.
June 24-26, 2000	**ARP0c2.c**	**Connection interceptor for switched networks which features ARP redirection/spoofing, automated bridging, automated routing, progressive attacks of known IP connections, network cleanup on exist and ARP flooding with random IP and Ethernet addresses.**
June 24-26, 2000	Iisdos.c	Denial of Service exploit against Microsoft Windows 2000 running IIS.
June 24-26, 2000	Nemesis-1.1.tar.gz	A commandline-based, portable human IP stack for Unix/Linux, which is broken down by protocol, and should allow for useful scripting of injected packet streams from shell scripts.
June 24-26, 2000	OffensiveUseofIDS.pdf	This paper explores ways that Intrusion Detection Systems (IDS) can be used for offensive purposes.
June 24, 2000	**Tpi.pl**	**Exploit script for the Netscape Professional Services FTP Server vulnerability.**
June 22-23, 2000	Bobek.c	Wu-Ftpd 2.6.0 remote root exploit script.
June 22-23, 2000	Hhp-ls.patch	Patch and one line Perl script for a local Denial of Service exploit via the '-w' parameter.
June 22-23, 2000	Inews_bof.c	Local buffer overflow exploit script for Inews (INN-2.2).
June 22-23, 2000	Wuftpd-2.6.0-exp2.c	Wu-Ftpd 2.6.0 remote root exploit script.
June 22-23, 2000	Wuftpd2600.c	Wu-Ftpd 2.6.0 remote root exploit script.
June 21, 2000	Swwpbof.c	Exploit script the WinProxy Buffer Overflow vulnerability.
June 19-21, 2000	Argo1002.pl	Exploit script, which causes Argosoft Mail Server 1.0.0.2 to page fault if the finger daemon is running.
June 19-21, 2000	Fbi-aim-dos.txt	AOL Instant Messenger remote Denial of Service exploit.
June 19-21, 2000	**Imesh102.pl**	**Buffer overflow exploit script for the iMesh 1.02 vulnerability which will allow for the execution of arbitrary code.**
June 19-21, 2000	Infosec.20000617.panda.a	Novell Netware servers running Panda Antivirus allows malicious users to run any command on a Netware console.
June 19-21, 2000	MacPork_3.0_PPC.sit	Macintosh based remote vulnerability scanner which scans for over 271 vulnerabilities and attempts to retrieve passwords in 175 different ways. It also detects 177 remote access Trojans.
June 19-21, 2000	**Netscape.ftp.txt**	**Exploit technique for the Netscape Professional Services FTP Server vulnerability.**
June 19-21, 2000	Porkbind-1.1.tar.gz	DNS server vulnerability scanner which retrieves the version of bind information for the nameservers and produces a report.
June 19-21, 2000	Testsyscall.c	Exploit script for the buffer overflow vulnerability in BSD, which allows for the execution of arbitrary commands.
June 19-20, 2000	**Life_Stages.txt**	**Life Stages worm .vbs source code.**
June 19-20, 2000	Userregsp.c	MailStudio2000 2.0 and below userreg.cgi exploit script which executes arbitrary commands on the remote host as root.mail.
June 16-18, 2000	**Dsniff-2.2.tar.gz**	**Suite of utilities that are useful for penetration testing.**
June 16-18, 2000	Pine_bof.c	Local buffer overflow exploit script for the Pine 4.10-21 vulnerability.
June 16-18, 2000	Saint-2.1.1.beta1.tar.gz	Security assessment tool based on SATAN model.
June 16-18, 2000	Sara-3.1.2.tar.gz	Security analysis tool based on the SATAN model.
June 16-18, 2000	Setconfxploit.c	Local root exploit script for Corel Linux 1.0 with xconf utils.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
June 16-18, 2000	Varitas.solaris.txt	Exploit technique for the Veritas Volume Manager 3.0.x vulnerability, which can, under specific circumstances, allow local malicious users to gain root access.
June 16-18, 2000	Winfingerprint-225.zip	Advanced remote Windows OS detection which does not run under Windows 9x.
June 16-18, 2000	Wmnetmon_bof.c	Buffer overflow exploit script for Linux.
June 16-18, 2000	Zodiac-0.4.9.tar.gz	Portable, extensible and multithreaded DNS tool.
June 15, 2000	**Access.vba.txt**	**Technique for exploiting Microsoft Access documents by inserting Trojan VBA code.**
June 15, 2000	Crash_winlogin.c	Proof-of-concept exploit for the Remote Registry Access Authentication vulnerability in Windows NT 4.0.
June 15, 2000	Splitexp.c	Local root buffer overflow exploit for the Splitvt 1.6.3 vulnerability.

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

No scripts were submitted during the two-week period covered by this issue of CyberNotes.

Trends

DDoS/DoS:

- A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attack.
- Continued reports of a combination of tools called "mstream." The purpose of the tool is to enable intruders to utilize multiple Internet connected systems to launch packet-flooding Denial of Service attacks against one or more target systems. An updated tool, findddos version 4.0, that allows users to identify the presence of mstream and other DDoS agents on host systems can be found on the NIPC website at http://www.nipc.gov/advis00-044.htm.

Probes/Scans:

- An increase to port 543/tcp (Kerberos authenticated services buffer overflow vulnerability).
- A continuation of scans to port 109 (pop2 exploit).
- A continuation of probes to UDP Port 137 (NetBIOS Name Service).
- Additional discussion concerning the AMDROCKS BIND exploit.
- Increasing reports of scans to known Trojan ports. System administrators should consult their intrusion detection system and firewall logs for unusual port scans.

Other:

- **The number of cases of infection caused by VBS/ShellScrap.Worm, alias 'VBS/Life_stages' and 'VBS.Stages Worm' is continuing to increase.**

- There have been a number of recent malicious programs exploiting the default behavior of Windows operating systems to hide file extensions from the user. This behavior can be used to trick users into executing malicious code by making a file appear to be something it is not. Multiple e-mail-borne viruses are known to exploit the fact that Microsoft Windows operating systems hide certain file extensions.
- Continuing compromises of systems running various vulnerable versions of BIND (including machines where the system administrator does not realize a DNS server is running).
- CERT has published several advisories concerning "Webpage Defacements on IIS Servers" and has posted two new server configuration guides. The "Securing Network Servers" guide can be found at http://www.cert.org/security-improvements/modules/m10.html. The "Securing Public Web Servers" can be found at http://www.cert.org/security-improvements/modules/m11.html.
- Certain virus e-mail gateways are reportedly not catching all virus signatures.
- A steady number of reports of intruders exploiting unprotected Windows networking shares.
- Reports indicate domain name registration information continues to be maliciously altered, including point of contact information for domain names, IP address delegations, and autonomous system numbers.

Viruses

VBS/Pica-A (Visual Basic Script Worm): This is a mass mailing worm that attempts to use Outlook and mIRC (Internet Relay Chat) to spread itself. The virus appears to have been written using a simple kit, allowing the message to have differing subject lines, body text and attachment filenames.

WM97/Antiv-A (Word 97 Macro Virus): This virus checks for macro module names in documents that are currently open. If the names are not "Hunter" or "ThisDocument," the virus displays a message box in Portuguese, informing the user that a document has been infected with a virus. It then displays a question asking whether a viral macro project should be removed. If the user answers yes, the virus removes the macro but also infects documents with its own viral macro. The name of the viral macro module is "Hunter." The virus repeats this action for each macro in each document that is open**.**

W97M/Chack.K (Word 97 Macro Virus): This virus uses stealth techniques and impedes displaying the dialog box that permits disabling macros in the document being opened.

W97M_Echa (Word 97 Macro Virus): This destructive macro virus has two payloads. After every execution it deletes all files in the default Word Application Start-Up folder. On March 5, the virus launches Office Assistant with a balloon message. This balloon message with a different name is also launched on August 8 and December 22.

WM97/Ethan-CZ (Word 97 Macro Virus): This is a simple Word macro virus, which contains just one macro. However, it can mix with other viruses to produce a double infection.

WM97/Fs-Q (Word 97 Macro Virus): This is a simple Word macro virus. It will replicate in any double-byte version of Word except Japanese.

WM97/Melissa-G (Word 97 Macro Virus and E-Mail Worm): This virus is a variant of WM97/Melissa and there have been several reports of it in the wild. On any day in January 2000, the virus edits the registry so that none of the drive icons appear in the Microsoft Explorer window.

WM97/Metys-D (Word 97 Macro Virus): There have been several reports of this virus in the wild. On September 18th, the virus displays a message box:

> "Happy Birthday Jess! To celebrate, we're going to see how lucky you are <Username>. Click the OK button below to roll a number. If your number matches that of the dealer, you win!"

If you win, the virus displays the message:

> "You roll a <number between 1 and 9> and the dealer rolls a<same number between 1 and 9>. You win!"

If you lose, the virus displays the message:

> "You roll a <number between 1 and 9> and the dealer rolls a <number between 1 and 9>. I'm sorry, but you lost. Better luck next time!"

The virus then adds the words "YOU LOSE!" to the beginning of the document.

W97M/Opey.M (Word 97 Macro Virus): This virus modifies the information about the user that Microsoft Word contains within the section "User Information" (accessed via the menu Tools - Options). It also changes document properties.

W97M_Osvald.B (Word 97 Macro Virus): This virus has been reported in the wild. While its payload does not delete files, it attempts to remove all spaces from infected documents.

W97M/RCH (Word 97 Macro Virus): This virus includes several stealth techniques that make detection by antiviral programs difficult as it impedes macros from being created or modified. In addition, on the 11th of every month, W97M/RCH activates its payload, which consists of displaying a dialog box with the following text: "Hoy es un buen día (user_name)."

WM97/Rendra-A (Word 97 Macro Virus): If the date is between April 3rd and May 10th, 2000 the virus displays a message box containing the following text:

> "Merci d'avoir utilise ce bel outil qu'est M.S. WORDS !!! Bill Gates vous le rendra!".

W97M_Sherlock (Word 97 Macro Virus): This non-destructive macro virus is encrypted and is triggered when an infected document is opened or closed. If its decryption function is removed, it cannot infect a document. Once triggered, this virus changes the application caption of the infected file. This macro virus employs an encryption on a portion of its code. The virus resides in the "ThisDocument" and is triggered when an infected document is opened or closed. It changes the application caption of an infected file to:

> "sherl0ck on the move" + <your document name>

WM97/Surround-B (Word 97 Macro Virus): This is a simple macro virus. If the day of the initial infection is the 21st of any month, the virus plays a beep sound.

WM97/Thursd-AB (Word 97 Macro Virus): This is a variant of WM97/Thursday. The virus will randomly choose a directory on a hard drive and copy the infected file to the directory. The name of the copied file will be identical to the name of an already existing file in the directory, but with the DOC extension. The virus also randomly chooses an existing file on the drive and corrupts it.

WM97/Thursd-AI (Word 97 Macro Virus): This is a variant of the WM97/Thursday virus. On the trigger date of December 13th it attempts to delete all files and subdirectories on the C: drive.

W97M/Thus.02 (Word 97 Macro Virus): The virus copies two files with TMP extensions containing the virus code into the folder containing the Microsoft Office 97 templates. The virus also tries to copy each of these files to a floppy disk. Additionally, the virus has a destructive payload that is activated on the 13th of December and consists in the deletion of all files in the hard disk; however, this routine is never actually executed.

WM97/Touchme-A (Word 97 Macro Virus): On March 5th, August 8th, and December 22nd, it launches the Office Assistant to display the message box "ReYoKh Team Labs mengucapkan Selamat Ulang Tahun !!!" and attempts to delete all files from the Word start-up path.

XM97/Divi-O (Excel 97 Macro Virus): This is an Excel spreadsheet macro virus, which creates a file called 874.XLS in the Excel template directory, and will infect other spreadsheets as they are opened or closed. The virus adds a flag, in the form of a variable called IVID plus a hexadecimal number, to each file as it is infected. This flag is used to determine whether the spreadsheet has already been infected.

XM/Totaler-B (Excel Macro Virus): On the May 11th, September 11th, October 29th, November 11th,

December 11th 1998, and November 2nd 1999, the virus attempts to delete all files from C:\WINDOWS\SYSTEM and C:\ directories. It also displays the message box "The NHS Fat Cow Has Just Trashed Your Hardisk."

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be updated on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	Issue discussed
Acid Shiver + lmacid	v1.0 + 1.0Mod	CyberNotes-2000-07
AOL Trojan		CyberNotes-2000-01
Asylum + Mini	v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1	CyberNotes-2000-10 (CyberNotes 2000-12)
AttackFTP		CyberNotes-2000-10
BF Evolution	v5.3.12	CyberNotes-2000-10
BioNet	v0.84 - 0.92 +2.2.1	CyberNotes-2000-09 (CyberNotes 2000-12)
Bla	1.0-5.02, v1.0-5.03	CyberNotes-2000-06, CyberNotes 2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
DeepThroat	v1.0 - 3.1 + Mod (Foreplay)	CyberNotes-2000-05
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
Drat	v1.0 - 3.0b	CyberNotes-2000-09
FakeFTP	Beta	CyberNotes-2000-02
GIP		CyberNotes-2000-11
Girlfriend	v1.3x (including Patch 1 & 2)	CyberNotes-2000-05
Golden Retreiver	v1.1b	CyberNotes-2000-10
Hack`a`Tack	1.0-2000	CyberNotes-2000-01, CyberNotes-2000-06
ICQ PWS		CyberNotes-2000-11
ik97	v1.2	CyberNotes-2000-07
InCommand	1.0-1.4, 1.5	CyberNotes-2000-01, CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-09, CyberNotes-2000-07
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes-2000-09, CyberNotes-2000-10
Intruder		CyberNotes-2000-01

Trojan	Version	Issue discussed
Kaos	v1.1 - 1.3	CyberNotes-2000-10
Khe Sanh	v2.0	CyberNotes-2000-10
Kuang Original	0.34	CyberNotes-2000-01
Magic Horse		CyberNotes-2000-10
Matrix	1.4-2.0, 1.0-2.0	CyberNotes-2000-01, CyberNotes-2000-09
MoSucker		CyberNotes-2000-06
Naebi	v2.12 - 2.39, v2.40	CyberNotes-2000-09 (CyberNotes 2000-12)
NetController	v1.08	CyberNotes-2000-07
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
NetTrojan	1.0	CyberNotes-2000-06
Nirvana / VisualKiller	v1.94 - 1.95	CyberNotes-2000-07
Omega		CyberNotes 2000-12
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	1.2-1.3	CyberNotes-2000-06
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65 – 0.70 b5	CyberNotes-2000-09 (CyberNotes 2000-12)
Revenger	1.0-1.5	CyberNotes 2000-12
Serbian Badman		CyberNotes 2000-12
Setup Trojan (Sshare) +Mod Small Share		CyberNotes-2000-06
ShadowPhyre	v2.12.38 - 2.X	CyberNotes-2000-06
ShitHeap		CyberNotes-2000-09
Snid	1-2	CyberNotes 2000-12
Softwarst		CyberNotes-2000-05
SubSeven	1.0-2.1c	CyberNotes-2000-01
SubSeven	1.0-2.1Gold	CyberNotes-2000-02
SubSeven	V1.0-1.9b, v2.1+SubStealth, v2.2b1	CyberNotes-2000-07
SubSeven	V2.1 Bonus	CyberNotes 2000-1
Trinoo		CyberNotes-2000-05
Troj/Simpsons		**Current Issue**
TryIt		CyberNotes-2000-05
wCrat	v1.2b	CyberNotes-2000-05
WinCrash	Beta	Current Issue
Winkiller		CyberNotes 2000-12

Troj/Simpsons (June 29, 2000): Troj/Simpsons is a self-extractable ZIP file called SIMPSONS.EXE, which contains the files SIMPSONS.BAT and SIMPSONS.BMP. The file icon has been altered so that it looks like an installation package.

When the executable file is run, it extracts the files and automatically runs SIMPSONS.BAT. This attempts to delete all files from drives A: to D: using the DELTREE command. If the DELTREE command is on one of the drives being deleted, then the Trojan will be unable to delete any further drives.

The payload does not function on standard Windows NT and Windows 2000 installations because DELTREE.EXE is not available.

SIMPSONS.BMP is not a bitmap image but a valid ZIP archive file containing the files README.TXT, FILE_ID.DIZ and SAMPLE.EXE. These files are not viral or malicious.